WE CLAIM:

1. A method for a decryptor to obtain a decryption key from a key release agent comprising:

a decryptor obtaining an encryption block comprising a data ciphertext requiring a decryption key to decrypt, the encryption block further comprising key related information associated with a first {public key, private key} pair, the encryption block further comprising a key ciphertext consisting of the decryption key encrypted by the first public key of the first {public key, private key} pair, the encryption block not including an ACD (access controlled decryption) block;

the decryptor generating a key release request containing the key ciphertext, and the key related information and outputting the key release request to the key release agent;

the decryptor receiving a key release response specifying the decryption key.

2. A method according to claim 1 further comprising the decryptor making the decryptor information available to the key release agent.

3. A method according to claim 1 further comprising the decryptor using the decryption key to decrypt the data ciphertext.

4. A method according to claim 2 wherein the decryptor making the decryptor information available to the key release agent comprises including the decryptor information in the key release request.

5. A method according to claim 2 wherein the decryptor making the decryptor information available to the key release

agent comprises the decryptor providing the decryptor information to the key release agent while establishing a secure connection with the key release agent.

6. A method according to claim 1 further comprising the decryptor making the decryptor information available to the key release agent by providing a decryptor identifier which may be used to look up decryptor attributes from a repository.

7. A method according to claim 1 wherein the key related information comprises a key pair identifier.

8. A method according to claim 1 further comprising:

before generating the key release request, the decryptor determining if the private key of the first {public key, private key} pair is available at the decryptor;

upon determining the private key of the first {public key, private key} pair is not available at the decryptor generating the key release request.

9. A method according to claim 1 further comprising:

decrypting at least a portion of the key release response containing an encrypted version of the decryption key using a private key of a second {public key, private key} pair to recover the decryption key.

10. A method according to claim 1 wherein the encryption block comprises a plurality of key related information associated with a respective plurality of first {public key, private key} pairs, and a respective plurality of key ciphertexts each consisting of the decryption key encrypted by the public key of a respective one of the plurality of first {public key, private key} pairs associated with the plurality of key related informations, the method comprising:

generating the key release request containing the plurality of key ciphertexts, and the associated plurality of key related information.

11. A method according to claim 10 further comprising:

before generating the key release request, determining if at least one private key of the plurality of first {public key, private key} pairs is available at the decryptor;

upon determining none of the private keys of the plurality of first {public key, private key} pairs is available at the decryptor generating the key release request.

12. A decryptor adapted to implement a method according to claim 1.

13. A key release method comprising:

receiving a key ciphertext and key related information in respect of a key used to encrypt the key ciphertext from a decryptor;

obtaining decryptor information in respect of the decryptor;

deciding based on the decryptor information and the key related information whether decryption of the key ciphertext is to be permitted.

14. A method according to claim 13 wherein the decryptor information is received from the decryptor together with the key ciphertext and key related information.

15. A method according to claim 13 wherein obtaining decryptor information comprises receiving the decryptor

information while establishing a secure connection with the decryptor.

16. A method according to claim 13 wherein obtaining decryptor information comprises:

receiving from the decryptor a decryptor identifier;

using the decryptor identifier to lookup decryptor attributes from a public repository, the decryptor identifier and decryptor attributes together constituting the decryptor information.

17. A method according to claim 13 further comprising:

using information in a certificate as the decryptor information.

18. A method according to claim 17 further comprising:

obtaining the certificate from a certificate repository.

19. A method according to claim 17 further comprising receiving the certificate together with the key ciphertext and key related information.

20. A method according to claim 13 wherein the decryptor information is an identity or role of the decryptor, an alias, or a claim of access rights or privilege, or some other attribute of the decryptor of a corresponding decrypting device or platform.

21. A method according to claim 13 wherein the key related information comprises a key pair identifier.

22. A method according to claim 13 further comprising:

decrypting the key ciphertext, re-encrypting the key using a public key of a {public key, private key} pair to produce a re-encrypted key, the private key of which is available to the decryptor, and sending the re-encrypted key to the decryptor.

23. A method according to claim 13 further comprising:

decrypting the key ciphertext to obtain a decryption key;

sending the decryption key to the decryptor over a secure channel.

24. A method according to claim 13 further comprising:

decrypting the key ciphertext to obtain a decryption key;

using a symmetric key available to the decryptor, encrypting the decryption key with the symmetric key to produce an encrypted decryption key, and sending the encrypted decryption key to the decryptor.

25. A method according to claim 13 further comprising:

receiving a plurality of key ciphertexts and respective key related information from the decryptor and determining whether at least one private key required to decrypt a respective at least one key ciphertext of the plurality of key ciphertexts is available;

upon determining such at least one private key is available, deciding based on the decryptor information whether decryption of at least one of the plurality of key ciphertexts is to be permitted.

26. A method according to claim 25 further comprising:

decrypting one of the key ciphertexts using a corresponding private key to recover a decryption key.

27. A method according to claim 25 wherein deciding based on decryptor information of the decryptor and the key related information whether decryption of at least one of the key ciphertexts is to be permitted comprises applying decryptor authorization logic associated with each public key used to encrypt the decryption key to the decryptor information to determine whether the decryptor should be permitted access to the decryption key.

28. A method according to claim 13 wherein deciding based on decryptor information of the decryptor and the key related information whether decryption of the key ciphertext is to be permitted comprises applying at least one rule associated with the public key used to encrypt the decryption key to the decryptor information to determine whether the decryptor should be permitted access to the decryption key;

29. A method of controlling access to a decryption key comprising:

receiving from a decryptor a key release request comprising decryptor information and the decryption key encrypted using a public key;

applying decryption authorization logic associated with the public key used to encrypt the decryption key to the decryptor information to determine whether the decryptor should be permitted access to the decryption key;

upon determining the decryptor should be permitted access to the decryption key, sending a key release response specifying the decryption key.

30. A method of controlling access to decryption keys comprising:

maintaining a private key repository comprising a plurality of access identifiers, and for each access identifier at least one key related information of a respective {public key, private key} pair, the repository also containing the private key of each {public key, private key} pair;

maintaining a repository comprising for each access identifier a respective decryptor authorization logic which can be applied to a decryptor information;

obtaining decryptor information;

receiving a key release request containing a decryption key encrypted using a public key of a {public key, private key} pair and containing a key related information associated with the {public key, private key} pair;

for each access identifier in association with which the key related information is stored, applying the respective decryptor authorization logic to the decryptor information specified in the key release request;

in the event the decryptor information satisfies at least one of the respective decryptor authorization logics, decrypting the ciphertext to recover the decryption key, and sending a key release response to the decryptor specifying the decryption key.

31. An administrative interface comprising:

a private key repository maintenance function adapted to allow adding and deleting of a key related information and associated private key of a {public key, private key} pair; and

a decryptor authorization logic definition function adapted to allow the definition of decryptor authorization logic to be applied to decryptor information to determine eligibility to decrypt, and for each decryptor authorization logic to select one or more of the key related information in respect of which the rule is to be applied.

32. An administrative interface according to claim 31 wherein the private key repository maintenance function is further adapted to store the key related information and associated private key of a {public key, private key} pair in association with one of a plurality of access identifiers;

and wherein the decryptor authorization logic definition function is further adapted to store each authorization logic in association with one of the plurality of access identifiers.

33. A decryptor comprising:

means for obtaining an encryption block comprising a data ciphertext requiring a decryption key to decrypt, the encryption block further comprising key related information associated with a first {public key, private key} pair, the encryption block further comprising a key ciphertext consisting of the decryption key encrypted by the first public key of the first {public key, private key} pair, the encryption block not including an ACD (access controlled decryption) block;

means for generating a key release request containing the key ciphertext, and the key related information and outputting the key release request to the key release agent;

means for receiving a key release response specifying the decryption key.

34. A decryptor according to claim 33 further comprising means for making the decryptor information available to the key release agent.

35. A decryptor according to claim 33 further means for using the decryption key to decrypt the data ciphertext.

36. A decryptor according to claim 33 adapted to make the decryptor information available to the key release agent by including the decryptor information in the key release request.

37. A decryptor according to claim 33 further comprising means for decrypting at least a portion of the key release response containing an encrypted version of the decryption key using a private key of a second {public key, private key} pair to recover the decryption key.

38. A key release agent comprising:

means for receiving from a decryptor a key ciphertext and key related information in respect of a key used to encrypt the key ciphertext;

means for obtaining decryptor information in respect of the decryptor;

means for deciding based on decryptor information of the decryptor and the key related information whether decryption of the key ciphertext is to be permitted.

39. A key release agent according to claim 38 adapted to receive the decryptor information together with the key ciphertext and key related information.

40. A key release agent according to claim 38 adapted to use the decryptor identifier to lookup decryptor attributes from a repository, the decryptor identifier and decryptor attributes together constituting the decryptor information.

41. A key release agent according to claim 38 further comprising:

decrypting means for decrypting the key ciphertext,

encryption means for re-encrypting the key using a public key of a {public key, private key} pair to produce a re-encrypted key, the private key of which is available to the decryptor;

means for sending the re-encrypted key to the decryptor.

42. A key release agent according to claim 38 further comprising:

decryptor authorization logic associated with each public key used to encrypt the decryption key to the decryptor information for determining whether the decryptor should be permitted access to the decryption key.